13. A method as claimed in claim 10, wherein said currently held data includes received e-mail messages.

14. A method as claimed in claim 10, wherein said step of scanning seeks to detect within said addressed data one or more of:

computer viruses;

worms;

Trojans;

banned computer programs;

banned words; or

banned images.

15. A method as claimed in claim 10, wherein said method is performed by a firewall computer via which internet traffic is passed to a local computer network.

16. A method as claimed in claim 10, wherein said addressed data is cached when it has been retrieved.

17. A method as claimed in claim 10, wherein if malware is detected within said addressed data, then one or more malware found actions are triggered.

18. A method as claimed in claim 10, wherein said malware found actions including at least one of:

(i) preventing access to said currently held data;

(ii) removing said at least one internet address from said currently held data;

(iii) preventing access to said addressed data;

(iv) removing said malware from said addressed data to generate clean addressed data and supplying said clean addressed data in place of said addressed data;

(v) blocking internet access by a computer detected to be seeking to access said at least one internet address.